September 2019-match BR version 1.6.6

CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs)

CA's Self-Assessment of CP/CPS documents to CA/Browser Forum Baseline Requirements (BRs) for SERPRO SSL AC – Government of Brazil

Introduction must include:
1) CA's Legal Name : Autoridade Certificadora do SERPRO SSL(AC SERPRO SSL)

2) The AC SERPRO SSL consists of a one-level CA hierarchy (See Graphic to the right):
- AC RAIZ: root-signing all issuing Cas certificate and kept offline.
- AC SERPRO SSL issuing restricted to only issue OV SSL certificates to domain names under ".gov.br ¨ level domain and owned by entities operating under the Brazilian Jurisdiction.
AC RAIZ:
SHA1 Fingerprint: 6C:15:5E:D7:27:1A:90:4A:0D:C0:40:F0:C8:57:FF:53:BF:6D:B2:90
SHA256 Fingerprint: 6E:0B:FF:06:9A:26:99:4C:15:DE:2C:48:88:CC:54:AF:84:88:2E:54:95:B7:FB:F6:6B:E9:CC:FF:EC:74:89:F6
AC SERPRO SSL:
SHA1 Fingerprint:0B:2F:DB:B1:A4:20:AB:99:79:23:BD:4F:E8:E3:3B:8B:BF:49:DD:94
SHA256 Fingerprint:08:FC:94:2D:51:76:E5:68:AC:BE:F9:C5:95:F3:6A:20:DE:6A:CF:9E:A3:0C:6F:5F:CE:DD:48:21:6E:D5:B0:70

3) List the specific version(s) of the used BR 1.6.6

4) CP/CPS documents:
CP/CPS Tuntrust PKI version 01 on 01 September 2019 : https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf
CP/CPS Tuntrust PKI version 02 on 28 April 2020: https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf
CP/CPS TunTrust PKI version 03 on 12 May 2020: https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf
CP/CPS TunTrust PKI version 3.1 on 01 June 2020: https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf

5) The current CP/CPS are up to date at to the BR 1.6.6.

BR Section Number	**List the specific documents and section numbers of those documents which meet the requirements of each BR section**	**Explain how the CA's listed documents meet the requirements of each BR section.**
1.2.1. Revisions Note the Effective Date for each item in the table. Certificates created after each Effective Date are expected to be in compliance with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	**CP/CPS 1.2**	
1.2.2. Relevant Dates Note the Compliance date for each item in the table. Those are the dates by which your CP/CPS and practices are expected to be updated to comply with the item. Make sure your CA is in compliance with each of these items. After careful consideration, *indicate if your CA is fully compliant with all items in the table, or clearly indicate action that your CA is taking to improve compliance.*	**CP/CPS 1.2**	
1.3.2. Registration Authorities Indicate whether your CA allows for Delegated Third Parties, or not. *Indicate which sections of your CP/CPS specify such requirements, and how the CP/CPS meets the BR requirements for RAs.*	**CP/CPS 1.3.2**	SERPRO SSL AC does not delegate the execution of Verification requirements to a Delegated Third Party. SERPRO SSL AC operates a registration authority, referred to in this document as SERPRO RA, where all registration procedures are directly executed by SERPRO RA personnel as described in CP/CPS Section 1.3.2. and 3.2
2.1. Repositories *Provide the direct URLs to the CA's repositories*	**CP/CPS 2.1**	http://certificados2.serpro.gov.br/lcr/ https://repositorio.serpro.gov.br/lcr/
2.2 Publication of information - RFC 3647 "Effective as of 31 May 2018, the Certificate Policy and/or Certification Practice Statement **MUST be structured in accordance with RFC 3647**."	**CP/CPS 1.1.4**	
2.2 Publication of information - CAA Effective as of 8 September 2017 ... CA's Certificate Policy and/ or Certification Practice Statement ... SHALL ... **clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue.**	**CP/CPS 2.2.1**	Prior to issuing SSL Certificates, SERPRO SSL AC checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued as specified in RFC 6844.SERPRO SSL Cas CAA issuer domain is "gov.br."

2.2. Publication of information - BR text "The CA SHALL publicly give effect to these Requirements and represent that it will adhere to the latest published version." --> ***Copy the specific text that is used into the explanation in this row. (in English)***	**CP/CPS 1.1.3** **CP/CPS 2.2.1** **CP/CPS 2.3.1**	SERPRO SSL AC conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document
2.2. Publication of information - test websites "The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired." --> ***List the URLs to the three test websites (valid, revoked, expired) for each root certificate under consideration. If you are requesting EV treatment, then the TLS cert for each test website must be EV.***	**CP/CPS 2.2.2 and Links to the test website are published on the repository.**	valid :https://active-repositorio.serpro.gov.br/ Revoked : https://revoked-repositorio.serpro.gov.br/ Expired : https://expired-repositorio.serpro.gov.br/
2.3. Time or frequency of publication "The CA SHALL ... **annually** update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements. Section 3.3 of Mozilla's Root Store Policy states: "CPs and CPSes MUST be reviewed and updated as necessary at least once every year, as required by the Baseline Requirements. **CAs MUST indicate that this has happened by incrementing the version number and adding a dated changelog entry**, even if no other changes are made to the document." *Indicate your CA's policies/practices to ensure that the BRs are reviewed regularly, and that the CA's CP/CPS is updated annually.*	**CP/CPS 2.3.1**	SERPRO SSL AC reviews its CP/CPS at least annually and makes appropriate changes so that AC SERPRO SSL operation remains accurate, transparent and complies with requirements listed in Section 8 of the CP/CPS .SERPRO SSL AC closely monitors CA/Browser Forum ballots and updates to the Baseline Requirements and implements updates to SERPRO SSL AC operations in a timely manner. New or modified versions of this CP/CPS, Subscriber Agreements, or Relying Party agreements are published within seven days after approval
2.4. Access controls on repositories *Acknowledge that all Audit, CP, CPS documents required by Mozilla's CA Certificate Policy and the BRs will continue to be made publicly available.*	**CP/CPS 2.4**	
3.2.2.1 Identity If the Subject Identity Information in certificates is to include the name or address of an organization, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	**CP/CPS 3.1.2**	SERPRO SSL AC is restricted to issue OV SSL certificates for domain names under Government of Brazil top-level domain "gov.br" owned by entities under the National Institute of Information Technology(https://www.gov.br/iti/pt-br) – Brazilian Jurisdiction.
3.2.2.2 DBA/Tradename If the Subject Identity Information in certificates is to include a DBA or tradename, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	**CP/CPS 3.2.2.2**	
3.2.2.3 Verification of Country If the subject:countryName field is present in certificates, *indicate how your CP/CPS meets the requirements in this section of the BRs.*	**CP/CPS 3.2.2.3**	SERPRO SSL AC verifies that the organization is in Brazilian jurisdiction. The country field is always set toBrazil ISOformat country code "BR". SERPRO SSL AC does not issue SSL certificates to organizations that are not under the National Institute of Information Technology (https://www.gov.br/iti/pt-br) – Brazilian Jurisdiction.
3.2.2.4 Validation of Domain Authorization or Control *Indicate which of the methods of domain validation your CA uses, and where this is described in your CP/CPS.* ***Section 2.2 of Mozilla's Root Store Policy states: "For a certificate capable of being used for SSL-enabled servers, the CA must ensure that the applicant has registered all domain(s) referenced in the certificate or has been authorized by the domain registrant to act on their behalf. This must be done using one or more of the methods documented in section 3.2.2.4 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.4 it is complying with. CAs are not permitted to use 3.2.2.5 (4) ("any other method") to fulfill the requirements of method 3.2.2.4.8 (IP Address)."***	**CP/CPS 3.1.2**	

3.2.2.4.1 Validating the Applicant as a Domain Contact For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.	SERPRO SSL AC does not use this method.	
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	SERPRO SSL AC does not use this method.	
3.2.2.4.3 Phone Contact with Domain Contact **CAs SHALL NOT perform validations using this method after May 31, 2019**. Completed validations using this method SHALL continue to be valid for subsequent issuance per the applicable certificate data reuse periods.	SERPRO SSL AC does not use this method.	
3.2.2.4.4 Constructed Email to Domain Contact If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	SERPRO SSL AC does not use this method.	
3.2.2.4.5 Domain Authorization Document "For certificates issued on or after August 1, 2018, **this method SHALL NOT be used** for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates."	SERPRO SSL AC does not use this method.	
3.2.2.4.6 Agreed-Upon Change to Website If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	**CP/CPS 3.2.7.2.1**	
3.2.2.4.7 DNS Change If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	SERPRO SSL AC does not use this method.	
3.2.2.4.8 IP Address If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	SERPRO SSL AC does not use this method.	
3.2.2.4.9 Test Certificate **"This method has been retired and MUST NOT be used."**	SERPRO SSL AC does not use this method.	
3.2.2.4.10. TLS Using a Random Number If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.* *This subsection contains major vulnerabilities.* ***If the CA uses this method, then the CA should describe how they are mitigating those vulnerabilities. If not using this method, the CPS should say so.***	SERPRO SSL AC does not use this method.	
3.2.2.4.11 Any Other Method **"This method has been retired and MUST NOT be used."**	SERPRO SSL AC does not use this method.	
3.2.2.4.12 Validating Applicant as a Domain Contact "This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name." If your CA uses this method of domain validation, *indicate where in the CP/CPS it is described, and how your CA meets the requirements in this section of the BRs.*	SERPRO SSL AC does not use this method.	

3.2.2.5 Authentication for an IP Address If your CA allows IP Addresss to be listed in certificates, ***indicate which methods your CA uses*** *and how your CA meets the requirements in this section of the BRs.* **Section 2.2 of Mozilla's root store policy says: "the CA must ensure that the applicant has control over all IP Address(es) referenced in the certificate. This must be done using one or more of the methods documented in section 3.2.2.5 of the CA/Browser Forum Baseline Requirements. The CA's CP/CPS must clearly specify the procedure(s) that the CA employs, and each documented procedure should state which subsection of 3.2.2.5 it is complying with."**	**CP/CPS 3.2.7.2.1**	
3.2.2.6 Wildcard Domain Validation If your CA allows certificates with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, then *indicate how your CA meets the requirements in this seciton of the BRs.*	**CP/CPS 3.2.7.2.1**	'
3.2.2.7 Data Source Accuracy *Indicate how your CA meets the requirements in this section of the BRs.*	**CP/CPS 4.2.1**	SERPRO SSL AC uses entities as data sources and third party databases sourced: https://transparencyreport.google.com/safe-browsing/search?url and https://registro.br/tecnologia/ferramentas/whois/ SERPRO SSL AC considers it a reliable data source
3.2.2.8 CAs MUST check and process CAA records *Indicate how your CA meets the requirements in this section of the BRs.* *Section 2.2 of the BRs states: "**CA's Certificate Policy and/or Certification Practice Statement ... shall clearly specify the set of Issuer Domain Names that the CA recognises in CAA "issue" or "issuewild" records as permitting it to issue."***	**CP/CPS 2.2**	Prior to issuing SSL Certificates,AC SERPRO SSL checks for CAA records for each dNSName in the subjectAltName extension of the Certificate to be issued as specified in RFC 6844. AC SERPRO SSL`s CAA issuer domain is "gov.br"
3.2.3. Authentication of Individual Identity	**CP/CPS 3.2.3**	
3.2.5. Validation of Authority	**CP/CPS 3.2.5**	
3.2.6. Criteria for Interoperation or Certification Disclose all cross-certificates in the CA hierarchies under evaluation.		SERPRO SSL AC does not have any cross-certificates with other CAs.
4.1.1. Who Can Submit a Certificate Application Indicate how your CA identifies suspicious certificate requests.	**CP/CPS 4.1.1**	[...] OV SSL certificates applications can only be submitted be through the SERPRO AR.
4.1.2. Enrollment Process and Responsibilities	**CP/CPS 4.1.2**	
4.2. Certificate application processing	**CP/CPS 4.2**	
4.2.1. Performing Identification and Authentication Functions *Indicate how your CA identifies high risk certificate requests.* **Re-use of validation information is limited to 825 days**	**CP/CPS 4.2.1**	The CA and RA perform the identification and authentication functions according to item 3 of this CPS. SERPRO SSL CA does not reuse previous validations. Each certificate request must go through all the validation functions described in section 3.2. Certificates issued by the CA are valid for 12 months. The CA maintains and implements procedures that are documented, identifying and making additional checks for high-risk certificate requests, prior to approval, ensuring that such requests are verified correctly under the requirements in the CA / Browser Forum, version 1.6.6, which cites Google's safe browsing list: https://transparencyreport.google.com/safe-browsing/search?url=www.bb.com.br&hl=pt_BR.
4.2.2. Approval or Rejection of Certificate Applications "Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA MUST (1) compare the new gTLD against the CA's records of valid certificates and (2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after the CA has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4. Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CAs MUST revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name."	**CP/CPS 4.2.2**	The CA and RA may, with due formal justification, accept or reject requests for certificates from applicants in accordance with the procedures described in this CPS.

4.3.1. CA Actions during Certificate Issuance	**CP/CPS 4.3.1 and 4.3.2**	4.3.1. CA actions while issuing a certificate 4.3.1.1. Certificates are issued by the CA according to the following steps: a) The person responsible for RA verifies the complete and correct completion of the certificate request, as well as the applicant's documentation; b) The person responsible for the RA approves the request, making the certificate available for installation by its applicant; c) The CA software automatically issues an email informing the applicant that the certificate is available for installation. 4.3.1.2. The certificate is considered valid from the moment of its installation 4.3.2. Notifications to the certificate holder by the CA when issuing the certificate The CA software automatically issues an email informing the applicant that the certificate is available for installation.

4.9.1.1 Reasons for Revoking a Subscriber Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking certificates.*	**CP/CPS 4.9.1**	4.9. Certificate Suspension and Revocation 4.9.1. Circumstances for revocation 4.9.1.1. The CA may revoke a certificate within 24 hours, issued by it, for one or all of the reasons listed: a) Revocation request correctly filled out by the Certificate Holder; b) Request for revocation sent to the CA by an authorized third party, for example, a court order; c) Request for revocation by a person with a certificate holder proxy; d) Certificate Holder leaves the community of interests under which his certificate was issued, for example: • Holder of an organizational certificate leaves the job; • The death of the Certificate Holder occurs; 4.9.1.2. A certificate must be revoked for the following reasons. a) When an improper or defective issue is found; b) When it is necessary to change any information contained therein; c) In case of dissolution of CA; or d) In case of compromise of the corresponding private key or its storage medium. 4.9.1.3. Regarding the revocation, it should also be noted that: a) The CA will revoke, within the period defined in item 4.9.3.3, the certificate of the entity that fails to comply with the policies, standards and rules established by ICP-Brasil; and b) The CG of ICP-Brasil or AC Raiz will determine the revocation of the certificate of the CA that fails to comply with the legislation in force or the policies, standards, practices and rules established by ICP-Brasil. c) The validation of the FQDN or the IP address is not in accordance with the established and cannot be used. d) The certificate does not comply with the requirements of items 6.1.5. and 6.1.6; e) The certificate was used incorrectly by the Certificate Holder, violating one of the obligations he signs in the Certificate Term; f) The CA becomes aware that an FQDN or an IP in a certificate is no longer legally permitted; g) The CA is informed that a wildcard certificate has been used to authenticate a fraudulent form of the domain; h) When the CA is aware of a material change in the information contained in the certificate; i) When the certificate has not been issued in accordance with the Requirements or the Certification Policy or Certification Practice Statement of that CA; j) The CA determines or is aware that any information displayed on the certificate is inaccurate; 4.9.1.4. Every certificate must have its validity verified, in the respective LCR, before being used. 4.9.1.4.1. The CA supports OCSP requests in accordance with RFC 6960 and / or RFC5019 and requirements of the document WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES. 4.9.1.4.2. The CA provides assurances that an LCR can be downloaded in no more than three seconds over an analog phone line, under a normal network condition. 4.9.1.5. The authenticity of the LCR must also be confirmed by verifying the signature of the issuing CA and the validity period of the LCR.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate *Indicate which section in your CA's CP/CPS contains the list of reasons for revoking subordinate CA certificates.*		SERPRO SSL AC does not have any third party Subordinate CAs.
4.9.2. Who Can Request Revocation	**CP/CPS 4.9.2**	4.9.2 Who can request revocation The request to revoke a certificate can only be made: a) at the request of the certificate holder; b) at the request of the person responsible for the certificate, in the case of a certificate of equipment, applications and legal entities; c) at the request of a company or body, when the holder of the certificate provided by that company or body is its employee, employee or servant; d) by the issuing CA; e) by a linked RA; f) by determination of the CG of ICP-Brasil or AC Raiz; h) By active civil servants and military personnel from the Union, States and the Federal District, authorized by the respective competent bodies for their identification
4.9.3. Procedure for Revocation Request	**CP/CPS 4.9.3**	4.9.3. Revocation request procedure 4.9.3.1. The procedure for requesting a revocation varies depending on who originates it and the CA will have up to 24 hours after the request to respond to the revocation. Certificate revocation requests can be made as follows and are available 24 x 7: a) Through the certificate request page under the option “Revoke”; b) Sending the specific form available on the certificate request page, filled in as the applicant's data and signed; c) For Fraud Report, through the service channels in item 1.5.2, “b”. 4.9.3.2. As general guidelines, it is established that: a) The applicant for revocation of a certificate will be identified; b) Revocation requests, as well as the actions resulting from them, will be registered and stored; c) The justifications for revoking a certificate are documented; and d) The process of revoking a certificate will end with the generation and publication of an LCR containing the revoked certificate. 4.9.3.3. The maximum time allowed for the completion of the certificate revocation process, after receiving the respective request, for all types of certificates provided for by ICP-Brasil is 24 (twenty four) hours. 4.9.3.4 Does not apply. 4.9.3.5. The CA is fully responsible for all damages caused by the use of a certificate in the period between the request for its revocation and the issuance of the corresponding LCR. 4.9.3.6. If specific revocation procedures are required for the implemented PC, they must be described in the PC, in the corresponding item.
4.9.5. Time within which CA Must Process the Revocation Request	**CP/CPS 4.9.4/4.9.5**	4.9.4.1. The revocation request must be immediate when the circumstances defined in item 4.9.1 are configured. 4.9.4.2. The CA establishes a period of 7 (seven) working days for the acceptance of the certificate requested by its holder, within which the revocation of the certificate may be requested without charging the tariff by the CA. 4.9.5. Time when the CA must process the revocation request In the case of a formally constituted request, in accordance with ICP-Brasil rules, the CA must process the revocation immediately after analyzing the request. Within 24 hours of receiving a certificate problem report, CA will investigate the facts and circumstances listed in that Report and provide a preliminary report to the certificate holder. After analyzing the facts and circumstances, the CA will notify the certificate holder and the period since receipt of the problem report will not exceed the period established in item 4.9.1.1. The date selected by the CA will consider the following criteria for evaluation: 1. The nature of the alleged problem (scope, context, severity, magnitude, risk of damage); 2. The consequences of the revocation (direct and collateral impacts on the holders); 3. The number of Problem Reports with Certificates that have already been received on a given certificate; 4. The entity that made the complaint (for example, a complaint by a bailiff or not, that a website is involved in illegal activities) and 5.Relevant legislation.

4.9.7. CRL Issuance Frequency *Indicate if your CA publishes CRLs. If yes, then please test your CA's CRLs.*	**CP/CPS 4.9.7**	4.9.7.1. The frequency of issuing CRLs referring to end-user certificates is 1 (one) hour. 4.9.7.2. The maximum frequency allowed for the issuance of LCR for end user certificates is 6 (six) hours.
4.9.9. On-line Revocation/Status Checking Availability	**CP/CPS 4.9.9**	The CA supports the online certificate status verification (OCSP) process. The online revocation process is available to the Certificate Holder, as described in item 3.4.
4.9.10. On-line Revocation Checking Requirements *Indicate how your CA meets all of the requirements listed in this section,* ***including support of GET, update frequency, preventing errounious return of "good" status.***	**CP/CPS 4.9.9 and 3.4**	
4.9.11. Other Forms of Revocation Advertisements Available Indicate if your CA supports OCSP stapling.	**CP/CPS 4.9.11**	SERPRO SSL AC does not employ any method other than OCSP and CRL for advertising revocation status.
4.10.1. Operational Characteristics	**CP/CPS 4.10.1**	4.10. Certificate status services 4.10.1. Operational characteristics The CA provides a certificate status service in the form of an LCR distribution point.
4.10.2. Service Availability	**CP/CPS 4.10.2**	See item 4.9.
5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS		
5.2.2. Number of Individuals Required per Task	**CP/CPS 5.2.2 and 6.2.2**	5.2.2. Number of people required per task 5.2.2.1. Multiuser control is required for the generation and use of the CA's private key, as described in 6.2.2. 5.2.2.2. All tasks performed in the environment where the CA certification equipment is located require the presence of at least 2 (two) operators (employees) of the CA. The other tasks of the CA can be performed by a single operator. 6.2.2. Control "n of m" for private key 6.2.2.1. The CA implements multiple control for the activation and deactivation of its private key through physical access controls and the certification software. 6.2.2.2. A minimum of 2 (two) holders of the activation key (“n”) from a group of 15 (fifteen) (“m”) is required to activate the CA key.
5.3.1. Qualifications, Experience, and Clearance Requirements	**CP/CPS 5.3.1 and 5.3.2**	All SERPRO SSL CA and related SERPRO AR personnel involved in activities directly related to the issuance, dispatch, distribution, revocation and certificate management processes are admitted as established in the CA Security Policy and the ICP-BRASIL SECURITY POLICY(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-02-v-3-1-polit-seg-da-icp-brasil-pdf) 5.3.2.1. In order to safeguard the security and credibility of the CA, all personnel involved in activities directly related to the processes of issuing, issuing, distributing, revoking and managing certificates, are subjected to the following processes, before the activities of: a) Criminal background check; b) Credit status check; c) Checking the history of previous jobs; and d) Proof of education and residence. 5.3.2.2. The CA may define additional requirements for background checks.
5.3.3. Training Requirements and Procedures	**CP/CPS 5.3.3**	5.3.3. Training requirements SERPRO SSL CA and linked SERPRO RA personnel involved in activities directly related to the issuing, shipping, distribution, revocation and certificate management processes receive documented training, with evidence at the end of the training when a concept is assigned that gives them mastery of the following themes: a) Principles and security mechanisms of CA and related RA; b) Certification system in use in the CA; c) Disaster recovery and business continuity procedures; d). Recognition of signatures and validity of the documents presented, in the form of item 3.2.2, 3.2.3. and 3.2.7; and e) Other matters relating to activities under its responsibility.
5.3.4. Retraining Frequency and Requirements	**CP/CPS 5.3.4**	5.3.4. Frequency and requirements for technical recycling All CA and RA related personnel involved in activities directly related to the processes of issuing, dispatching, distributing, revoking and managing certificates are kept up to date on any technological changes in the CA or RA certification system.
5.3.7. Independent Contractor Controls	**CP/CPS 5.3.7**	5.3.7. Requirements for hiring staff The personnel of the SERPRO SSL CA and the linked SERPRO RA, in the exercise of activities directly related to the processes of issuance, dispatch, distribution, revocation and management of certificates, are hired as established in the SECURITY POLICY OF ICP-BRASIL(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-02-v-3-1-polit-seg-da-icp-brasil-pdf).

5.4.1. Types of Events Recorded *Indicate how your CA meets the requirements of this section.*	**CP/CPS 5.4.1**	5.4.1. Registered Event Types 5.4.1.1. All actions performed by SERPRO SSL CA personnel, in the performance of their duties, are recorded so that each action is associated with the person who performed it. The CA records in files for auditing purposes all events related to the security of its certification system, which are: a) Initiation and termination of the certification system; b) Attempts to create, remove, set passwords or change system privileges for CA operators; c) Changes in the configuration of the CA or its keys; d) Changes in certificate creation policies; e) Attempts to access (login) and exit the system (logoff); f) Unauthorized attempts to access system files; g) Generation of CA's own keys or keys of end users; h) Issuing and revoking certificates; i) Generation of LCR, certificate revocation lists and OCSP directory entry; j) Attempts to initiate, remove, enable and disable users of systems and to update and recover their keys; k) Failed operations of writing or reading in the certificate and LCR repository, when applicable; and l) Write operations in this repository, when applicable. 5.4.1.1.1. This CA has the possibility to audit up to 6% of the SSL certificates issued. 5.4.1.2. The CA records, electronically or manually, security information not directly generated by its certification system, which are: a) Records of physical accesses; b) Maintenance and changes in the configuration of your systems; c) Changes in qualified personnel and profiles; d) Discrepancy and commitment reports; and e) Records of destruction of storage media containing cryptographic keys, certificate activation data or personal information of users. 5.4.1.3. The minimum audit records to be maintained by the CA include in addition to the above: a) Application records, including records relating to rejected applications; b) Certificate generation requests, even if the generation is not successful; c) LCR issuance request records. 5.4.1.4. All audit records, electronic or manual, contain the date and time of the recorded event and the identity of the agent that caused it. 5.4.1.5. To facilitate the audit processes, all documentation related to the CA services is stored, either electronically or manually, in a single location, in accordance with ICP-BRASIL'S SECURITY POLICY(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-02-v-3-1-polit-seg-da-icp-brasil-pdf. 5.4.1.6. The SERPRO AR linked to SERPRO SSL AC, by CPS, electronically records in audit files, all events related to the validation and approval of the request, as well as to the revocation of certificates. The following events included in audit files: a) The registry agents who performed the operations; b) Date and time of operations; c) The association between the agents that carried out the validation and approval and the certificate generated; d) The digital signature of the performer. 5.4.1.7. The CA stores, electronically, copies of documents for identification, presented at the time of requesting and revoking certificates and terms of ownership.
5.4.3. Retention Period for Audit Logs	**CP/CPS 5.4.3**	The CA maintains its audit records locally for at least 2 (two) months at SERPRO facilities and subsequently stores them in the manner described in item 5.5.
5.4.8. Vulnerability Assessments *Indicate how your CA meets the requirements of this section.*	**CP/CPS 5.4.8**	SERPRO SSL CA is ISO 27001:2013 certified by the certification authority APCER for all its services, solutions and activities; and in CPS: 5.4.8. Vulnerability assessments Events that indicate possible vulnerability, detected in the periodic analysis of the CA audit records, are analyzed in detail and, depending on their severity, recorded separately. Resulting corrective actions are implemented and recorded for audit purposes. In addition, the CA's security program includes an annual Risk Assessment that: 1. Identifies foreseeable internal and external threats that may result in unauthorized access, disclosure, misuse, alteration or destruction of any certificate data or in the certificate's own life cycle; 2. Evaluates the probability and possible damage of these threats, taking into account the sensitivity of the certificate data and the management process of the same; and 3. Evaluates the policies, procedures, information systems, technology and other agreements that the CA has to combat these threats.

5.5.2. Retention Period for Archive	**CP/CPS 5.5.2**	5.5.2. Retention period for archiving The retention periods for each archived record are as follows: a) CRLs referring to digital signature certificates are permanently retained for historical consultation purposes. b) The dossiers of the holders must be retained, at least, for 7 (seven) years, counting from the date of expiration or revocation of the certificate; and c) Other information, including audit files, must be retained for at least 7 (seven) years.
5.7.1. Incident and Compromise Handling Procedures *Indicate how your CA meets the requirements of this section.*	**CP/CPS 5.7.1**	5.7. Commitment and Disaster Recovery The CA declares that the requirements related to the notification and disaster recovery procedures are described in the AC Business Continuity Plan - as established in the SECURITY POLICY OF ICP-BRASIL(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-02-v-3-1-polit-seg-da-icp-brasil-pdf., guaranteeing the continuity of its critical services . 5.7.1. Incident management and commitment procedures 5.7.1.1. The Business Continuity Plan (PCN), is of restricted access, tested at least once a year, ensuring the continuity of critical services. It also has the Incident Response Plan (PRI) and Disaster Recovery Plan (PRD). The PCN, PRD and PRI are available for verification by the Qualified Auditors, when requested. 5.7.1.2. The procedures in the Business Continuity Plan (PCN) of the AR SERPRO linked to recover, in whole or in part, the activities of the AR, are as follows: a) Identification of events that may cause interruptions in business processes, for example equipment failure, floods and fires, if applicable; b) Identification and agreement of all responsibilities and emergency procedures; c) Implementation of emergency procedures that allow recovery and restoration within the necessary timeframes. d) Documentation of agreed processes and procedures; e) Adequate training of personnel in the defined emergency procedures and processes, including crisis management; and f) Test and update plans.
6.1.1. Key Pair Generation	**CP/CPS 6.1.1**	A qualified Webtrust auditor was present during the CA key pairs generations.
6.1.2. Private Key Delivery to Subscriber	**CP/CPS 6.1.2**	Applicants are solely responsible for the generation of the private keys used in their Certificate Requests. SERPRO SSL AC does not provide SSL key generation, escrow, recovery or backup operations.
6.1.5. Key Sizes	**CP/CPS 6.1.5**	6.1.5. Key sizes 6.1.5.1. The size of the cryptographic keys associated with the certificates issued by the CA is, at least, 2048 (two thousand and forty-eight) bits;
6.1.6. Public Key Parameters Generation and Quality Checking	**CP/CPS 6.1.6**	The parameters for the generation and verification of asymmetric keys of the end user adopt the standard established in the document ICP-BRASIL STANDARDS AND CRYPTOGRAPHIC ALGORITHMS(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-01-01-v-4-2-padroes-e-algoritmos-criptograficos-da-icp-brasil-copy-pdf)
6.1.7. Key Usage Purposes	**CP/CPS 6.1.7**	6.1.7. Purpose of using a key (according to the “Key usage” field in X.509 v3) 6.1.7.1. Certificates issued by the CA have “Digital usage” (2.5.29.15) in the digitalSignature and keyAgreement bits. The purposes for which the cryptographic keys of the certificate holders issued by the CA can be used, as well as the possible restrictions applicable in accordance with the applications defined for the corresponding certificates, are specified on each PC that it implements. 6.1.7.2. The CA's private key is used only for the signature of the certificates issued by it and its LCRs.
6.2. Private Key Protection and Cryptographic Module Engineering Controls	**CP/CPS 6.2**	The CA's private key is generated, stored and used only on specific cryptographic hardware, therefore there is no traffic at any time.
6.2.5. Private Key Archival	**CP/CPS 6.2.5**	6.2.5.1. The private keys of the certificate holders issued by the CA are not archived. 6.2.5.2. Archiving is defined as storing the private key for future use, after the period of validity of the corresponding certificate.
6.2.6. Private Key Transfer into or from a Cryptographic Module	**CP/CPS 6.2.6**	The CA's private key is inserted into the cryptographic module in accordance with RFC 4210 and 6712.

6.2.7. Private Key Storage on Cryptographic Module	**CP/CPS 6.2.7**	The CA key pair is generated by the CA itself, in a cryptographic hardware module with FIPS 140-1 level 3 security standard, using RSA algorithm for generating the key pair and 3-DES algorithm for its protection, after the approval of the request for accreditation and the subsequent authorization to operate within the scope of ICP-Brasil. The generation is through a ceremony with the participation of CA personnel with a reliable function to execute the key generation script and the participation of qualified auditors. 6.1.1.2. Key pairs are generated only by the corresponding Certificate Holder. The specific procedures are described in each implemented CP.
6.3.2 Certificates issued after March 1, 2018, MUST have a Validity Period no greater than 825 days *Indicate how your CA meets the requirements of this section.*	**CP/CPS 6.3.2**	The private key of the CA and the certificate holders issued by it are used only during the period of validity of the corresponding certificates. The public key of the CA can be used for the entire period of time determined by the applicable legislation, to verify signatures generated during the validity period of the corresponding certificate. 6.3.2.2. Not applicable. 6.3.2.3. Type A1 certificates, provided for in this PC, are valid for up to 1 year
6.5.1. Specific Computer Security Technical Requirements **The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.** *Indicate how your CA meets the requirements of this section.*	**CP/CPS 6.5.1**	6.5.1. Specific technical requirements for computer security 6.5.1.1. The CA ensures that the generation of its key pair is performed in an offline environment, to prevent unauthorized remote access. 6.5.1.2. The general requirements for computational security of the equipment where the cryptographic key pairs of the certificate holders issued by the CA are generated are described in the implemented PC. 6.5.1.3. The server computers used by the CA, directly related to the processes of issuing, issuing, distributing, revoking or managing certificates, implement, among others, the following characteristics: a) Control of access to CA services and profiles; b) Clear separation of tasks and attributions related to each qualified profile of the CA; c) Restricted access to the CA databases; d) Use of encryption for database security, when required by the classification of your information; e) Generation and storage of CA audit records; f) Internal security mechanisms to guarantee the integrity of data and critical processes; and g) Mechanisms for backup copies (backup). 6.5.1.4. These characteristics are implemented by the operating system or by combining it with the certification system and with physical security mechanisms. 6.5.1.5. Any equipment, or part of it, when sent for maintenance has the sensitive information contained therein erased and input and output control is carried out, recording the serial number and the dates of sending and receiving. Upon returning to the facilities where the equipment used to operate the AC resides, the equipment that has undergone maintenance is inspected. In all equipment that is no longer used permanently, all stored sensitive information relating to the activity of the CA is permanently destroyed. All of these events are recorded for audit purposes. 6.5.1.6. Any equipment incorporated into the CA is prepared and configured as provided for in the implemented security policy or in another applicable document, in order to present the level of security necessary for its purpose.
7.1. Certificate profile **CAs SHALL generate non-sequential Certificate serial numbers greater than 0 containing at least 64 bits of output from a CSPRNG.** *Indicate how your CA meets the requirements of this section.*	**CP/CPS 7.1**	7.1. Certificate Profile All certificates issued by SERPRO SSL AC are in accordance with the format defined by the ITU X.509 or ISO / IEC 9594-8 standard, according to the profile established in RFC 5280..
7.1.1. Version Number(s)	**CP/CPS 7.1**	All certificates issued by the CA, according to CP, implement version 3 of the certificate defined in the ITU X.509 standard, according to the profile established in RFC 5280

7.1.2. Certificate Content and Extensions; Application of RFC 5280	**CP/CPS 7.1.2**	7.1.2. Certificate extensions 7.1.2.1. In this item, the PC describes all the certificate extensions used and their criticality. 7.1.2.2. ICP-Brasil defines the following extensions as mandatory: a) “Authority Key Identifier”, non-critical: contains the SHA-1 hash of the CA's public key; b) "Key Usage", critical: configured as provided in item 7.1.2.7 of this document; c) “Certificate Policies”, non-critical: contains the PC's OID 2.16.76.1.2.1.105 and the URL address of the website https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf with the DPC of B.C; Server authentication certificates (SSL / TLS) must also contain the OID of the CA / B Forum Guidelines requirements certificate policy (OV SSL = 2.23.140.1.2.2). d) “CRL Distribution Points”, non-critical: contains the URL address of the web page where the AC LCR is obtained: http://repositorio.serpro.gov.br/lcr/acserprosslv1.crl http://certificados2.serpro.gov.br/lcr/acserprosslv1.crl e) “Authority Information Access”, does not criticize, containing the id-ad-calssuer access method, using the HTTP access protocol for the recovery of the certification chain at the following address: http://repositorio.serpro.gov.br /strings/serprossl.p7b The second entry contains the access method id-ad-ocsp, with the respective address http://ocsp.serpro.gov.br/acserprosslv1 of the OCSP responder, using the access protocol, HTTP. 7.1.2.3. ICP-Brasil also defines the non-critical "Subject Alternative Name" extension as mandatory, with the following formats: c) For equipment or application certificate: c.1) 4 (four) otherName fields, mandatory, containing, in this order: i. OID = 2.16.76.1.3.8 and content = business name in the CNPJ (National Register of Legal Entities), without abbreviations, if the certificate is a legal entity; ii. OID = 2.16.76.1.3.4 and content = in the first 8 (eight) positions, the date of birth of the person responsible for the certificate, in the format ddmmaaaa; in the 11 (eleven) subsequent positions, the person's Individual Taxpayer Registration (CPF); in the 11 (eleven) subsequent positions, the Social Identification number - NIS (PIS, PASEP or CI); in the 15 (fifteen) subsequent positions, the RG number of the person responsible; in the 10 (ten) subsequent positions, the abbreviations of the RG issuing agency and the respective UF. iii. OID = 2.16.76.1.3.2 and content = name of the person responsible for the certificate; iv. OID = 2.16.76.1.3.3 and content = in the 14 (fourteen) positions the number of National Register of Legal Entities (CNPJ), if the certificate is for individuals legal; c.2) For certificates of type SSL / TLS, Field dNSName, mandatory, containing one or more domains owned or controlled by the holder, following the rules defined in RFC 5280 and RFC 2818, and in accordance with the WebTrust principles and criteria [6] and the CA / Browse Forum requirements [7]. 7.1.2.4. All fields and extensions in the AC SERPRO SSL certificates are defined according to RFC 5280. The “otherName” fields defined as mandatory by ICP-Brasil must comply with the following specifications: a) Information set defined in each otherName field must be stored as a string of type ASN.1 OCTET STRING or PRINTABLE STRING; b) When the CPF, NIS (PIS, PASEP or CI), RG, CNPJ, CEI, or Voter Registration numbers are not available, the corresponding fields must be completely filled in with "zero" characters; c) If the RG number is not available, the issuing agency and UF field should not be filled out. The same occurs for the municipality and UF field, if there is no registration number for the voter registration; d) Not applicable; e) All information of variable size referring to numbers, such as RG, must be filled with "zero" characters to its left so that the maximum possible size is completed; f) The 10 (ten) positions of the information about the issuing body of the RG and UF refer to the maximum size, and only the positions necessary for its storage, from left to right, should be used. The same applies to the 22 (twenty-two) positions of the information on municipality and UF of the Title of Voter; g) Only the characters A to Z and 0 to 9 can be used, and special characters, symbols, spaces or any other are not allowed. 7.1.2.5. Additional otherName fields, containing specific information and form of filling and storage defined by the CA, may be used with OIDs assigned or approved by the Root CA. 7.1.2.6. The other fields that make up the "Subject Alternative Name" extension may be used, in the form and for the purposes defined in RFC 5280. 7.1.2.7. The CA implements the following extensions, defined as mandatory by ICP-Brasil. a) Does not apply. b) for Server Authentication certificates (SSL / TLS): “Key Usage”, critical: only the digitalSignature and keyAgreement bits are activated; “Extended Key Usage”, not critical: contains the purpose of server authentication OID = 1.3.6.1.5.5.7.3.1, and also the purpose: client authentication OID = 1.3.6.1.5.5.7.3.2;

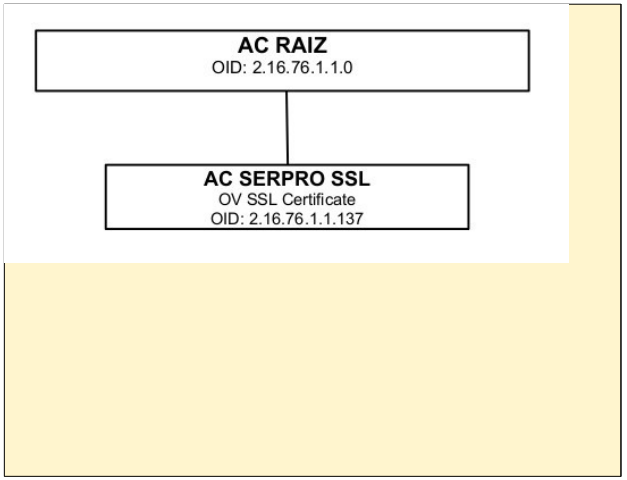
7.1.2.1 Root CA Certificate	**CPS 7.1.2.1 Certification Practices Statement by the Root Certification Authority of ICP-Brasil https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc**	The Root CA certificate implements the following extensions provided for in version 3 of the ITU-T X.509 standard: a) basicConstraints: contains the field cA = True. The pathLenConstraint field is not used. b) keyUsage: contains only the linked keyCertSign (5) and cRLSign (6) bits. The other bits are turned off. c) cRLDistributionPoints: contains the web address where the corresponding LCR is obtained to the certificate: For V10 chain certificates: http://acraiz.icpbrasil.gov.br/LCRacraizv10.crl d) Certificate Policies: specifies the Root CA's DPC Object Identifier (OID) and the attribute id-qt-cps with the web address of this DPC L (http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf). e) SubjectKeyIdentifier: contains the root CA's public key hash.
7.1.2.2 Subordinate CA Certificate	**CPS 7.1.2.2 Certification Practices Statement by the Root Certification Authority of ICP-Brasil https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc**	The level CA certificate immediately following that of the Root CA can implement any of the extensions provided for in version 3 of the ITU-T X.509 standard. The following extensions are mandatory: a) “Authority Key Identifier”, non-critical: the keyIdentifier field must contain the hash, obtained with algorithm of the SHA family, of the public key of the CA that issues the certificate; b) “Subject Key Identifier”, non-critical: it must contain the hash, obtained with the family algorithm SHA, the public key of the certificate holder CA; c) “Key Usage”, critical: the keyCertSign and cRLSign bits must be activated, which can be other bits are activated for specific cases; d) “Certificate Policies”, non-critical: d.1) the policyIdentifier field must contain: i. if the CA issues certificates to other CAs, the DPC OID of the CA holding the certificate; or ii. if the CA issues certificates to end users, the OIDs of the deployed PCs, containing the policyQualifiers field with the id-qt-cps attribute and the DPC web address of the CA; e) “Basic Constraints”, critical: must contain the field cA = True; and f) “CRL Distribution Points”, non-critical: must contain a web address where the LCR is obtained corresponding to the certificate, according to item 7.1.2.1.c.
7.1.2.3 Subscriber Certificate	**CP/CPS 7.1.2.3**	7.1.2.3. ICP-Brasil also defines the non-critical "Subject Alternative Name" extension as mandatory, with the following formats: c) For equipment or application certificate: c.1) 4 (four) otherName fields, mandatory, containing, in this order: i. OID = 2.16.76.1.3.8 and content = business name in the CNPJ (National Register of Legal Entities), without abbreviations, if the certificate is a legal entity; ii. OID = 2.16.76.1.3.4 and content = in the first 8 (eight) positions, the date of birth of the person responsible for the certificate, in the format ddmmaaaa; in the 11 (eleven) subsequent positions, the person's Individual Taxpayer Registration (CPF); in the 11 (eleven) subsequent positions, the Social Identification number - NIS (PIS, PASEP or CI); in the 15 (fifteen) subsequent positions, the RG number of the person responsible; in the 10 (ten) subsequent positions, the abbreviations of the RG issuing agency and the respective UF. iii. OID = 2.16.76.1.3.2 and content = name of the person responsible for the certificate; iv. OID = 2.16.76.1.3.3 and content = in the 14 (fourteen) positions the number of National Register of Legal Entities (CNPJ), if the certificate is for individuals legal; c.2) For certificates of type SSL / TLS, Field dNSName, mandatory, containing one or more domains owned or controlled by the holder, following the rules defined in RFC 5280 and RFC 2818, and in accordance with the WebTrust principles and criteria [6] and the CA / Browse Forum requirements

7.1.2.4 All Certificates	**CP/CPS 7.1.2.4**	7.1.2.4. All fields and extensions in the AC SERPRO SSL certificates are defined according to RFC 5280. The “otherName” fields defined as mandatory by ICP-Brasil must comply with the following specifications: a) Information set defined in each otherName field must be stored as a string of type ASN.1 OCTET STRING or PRINTABLE STRING; b) When the CPF, NIS (PIS, PASEP or CI), RG, CNPJ, CEI, or Voter Registration numbers are not available, the corresponding fields must be completely filled in with "zero" characters; c) If the RG number is not available, the issuing agency and UF field should not be filled out. The same occurs for the municipality and UF field, if there is no registration number for the voter registration; d) Not applicable; e) All information of variable size referring to numbers, such as RG, must be filled with "zero" characters to its left so that the maximum possible size is completed; f) The 10 (ten) positions of the information about the issuing body of the RG and UF refer to the maximum size, and only the positions necessary for its storage, from left to right, should be used. The same applies to the 22 (twenty-two) positions of the information on municipality and UF of the Title of Voter; g) Only the characters A to Z and 0 to 9 can be used, and special characters, symbols, spaces or any other are not allowed.
7.1.2.5 Application of RFC 5280	**CP/CPS 7.1.2.5 e 7.1.2.6.**	7.1.2.5. Additional otherName fields, containing specific information and form of filling and storage defined by the CA, may be used with OIDs assigned or approved by the Root CA. 7.1.2.6. The other fields that make up the "Subject Alternative Name" extension may be used, in the form and for the purposes defined in RFC 5280.
7.1.3. Algorithm Object Identifiers	**CP/CPS 7.1.3**	7.1.3.1. The cryptographic algorithms used for signing the certificates by the AC are those admitted within the scope of ICP-Brasil, according to ICP-BRASIL STANDARDS AND CRYPTOGRAPHIC ALGORITHMS(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-01-01-v-4-2-padroes-e-algoritmos-cri); 7.1.3.1.1. Certificates issued by the CA are signed using the SHA-256 cryptographic algorithm with a hash function (OID = 1.2.840.113549.1.1.11).
7.1.4. Name Forms	**CP/CPS 7.1.4**	7.1.4. Name formats The name of the certificate holder, included in the “Subject” field, must adopt the “Distinguished Name” (DN) of the ITU X.500 / ISO 9594 standard.
7.1.4.1 Issuer Information	**CP/CPS 7.1.4.1**	7.1.4.1. C = BR; O = ICP-Brasil; OU = name of the issuing CA; OU = CNPJ of the AR that performed the face-to-face identification; OU = Type of identification used (in person, video conference or digital certificate); CN = name of the certificate holder in an individual certificate;
7.1.4.2 Subject Information - Subscriber Certificates Section 7.1.4.2.1 states: Certificate Field: extensions:**subjectAltName** Required/Optional: Required Contents: **This extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.** Wildcard FQDNs are permitted. Section 7.1.4.2.2 states: Certificate Field: subject:commonName (OID 2.5.4.3) Required/Optional: Deprecated (Discouraged, but not prohibited) Contents: **If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate’s subjectAltName extension** (see Section 7.1.4.2.1).	**CP/CPS 7.1.4.2**	7.1.4.2. The digital certificate issued for server authentication (SSL / TLS) adopts the “Distinguished Name” (DN) of the ITU X.500 / ISO 9594 standard, as follows: CN = ccd.serpro.gov.br OU = SERPRO SSLv1 Certification Authority OU = ARSERPRO OU = Equipment A1 O = SERPRO - FEDERAL DATA PROCESSING SERVICE L = BRASILIA S = DF C = BR SERIALNUMBER = 33683111000107 1.3.6.1.4.1.311.60.2.1.3 = BR 2.5.4.15 = Business Entity
7.1.4.3 Subject Information - Root Certificates and Subordinate CA Certificates		

7.1.5. Name Constraints ***Indicate your CA's understanding of section 5.3 of Mozilla's root store policy, and requirement to disclose in the CCADB all subordinate CA certificates that are not technically constrained as described in this section of the BRs.*** ***"All certificates that are capable of being used to issue new certificates, that are not technically constrained, and that directly or transitively chain to a certificate included in Mozilla's root program:*** ***MUST be audited in accordance with Mozilla's Root Store Policy. ...*** ***MUST be publicly disclosed in the CCADB by the CA that has their certificate included in Mozilla's root program. The CA with a certificate included in Mozilla's root program MUST disclose this information within a week of certificate creation, and before any such subordinate CA is allowed to issue certificates. ..."***	**CP/CPS 7.1.5**	ICP-Brasil establishes the following restrictions on names, applicable to all certificates: a) accent marks, umlauts or cedillas should not be used; and b) in addition to the alphanumeric characters, only the following special characters may be used: see table inCP 7.1.5.
7.1.6. Certificate Policy Object Identifier	**CP/CPS 7.1.6**	7.1.6. Certificate Policy Object Identifier (OID) The OID assigned to this Certificate Policy is: 2.16.76.1.2.1.105. Every certificate issued under this PC must contain, in the "Certificate Policies" extension, the corresponding OID.
7.1.6.1 Reserved Certificate Policy Identifiers	**CP/CPS 7.1.2.2. c)**	Server authentication certificates (SSL / TLS) must also contain the OID of the CA / B Forum Guidelines requirements certificate policy (OV SSL = 2.23.140.1.2.2).
7.1.6.2 Root CA Certificates		Root CA certificates do not contain any certificatePolicies extension, therefore do not have policy identifiers in them.
7.1.6.3 Subordinate CA Certificates		Not apply for SERPRO SSL CA;
7.1.6.4 Subscriber Certificates		
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS		
8.1. Frequency or circumstances of assessment **The period during which the CA issues Certificates SHALL be dividied into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.** For new CA Certificates: The point-in-time readiness assessment SHAL be completed no earlier than twelve months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate. *Indicate your CA's understanding of this requirement, and how your CA meets the requirements of this section.*	**CP/CPS 8.1**	The CA undergoes prior auditing, for accreditation purposes, and annual audits, for accreditation maintenance purposes. Based on the requirements of the CA / Browser Forum, an annual audit is carried out by an independent external auditor to assess the CA's compliance with the established requirements. An audit period should not exceed one year.
8.2. Identity/qualifications of assessor *Indicate how your CA meets he requirements of this section.*	**CP/CPS 8.2**	8.2.1. The inspections of the CA are carried out by AC Raiz, through its own staff, at any time, without prior notice, observing the provisions in the document CRITERIA AND PROCEDURES FOR SUPERVISION OF THE INTEGRATING ENTITIES OF ICP-BRASIL(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-08-v-4-7-critrios-e-procedimen) 8.2.2. With the exception of the audit of AC Raiz itself, which is the responsibility of the CG of ICP-Brasil, the audits of ICP-Brasil members are carried out by AC Raiz, through its own staff, or by third parties authorized by it , in compliance with the provisions of the document CRITERIA AND PROCEDURES FOR CARRYING OUT AUDITS AT INTEGRATING ENTITIES OF ICP-BRASIL(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-08-v-4-7-critrios-e-procedimen)

8.4. Topics covered by assessment	**CP/CPS 8.4**	8.4.1. Inspections and audits carried out within the scope of ICP-Brasil aim to verify that the processes, procedures and activities of the entities that are part of ICP-Brasil are in compliance with their respective DPCs, PCs, PSs and other rules and procedures established by ICP-Brasil and with the principles and criteria defined by WebTrust [14], as well as the basic requirements of the CA / Browse Forum. 8.4.2. The CA received a prior audit from AC Raiz for the purposes of accreditation at ICP-Brasil and which is audited annually, for the purpose of maintaining accreditation, based on the provisions of the document CRITERIA AND PROCEDURES FOR CARRYING OUT AUDITS AT ICP-BRAZIL'S ENTITIES(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-08-v-4-7-critrios-e-procedimer). This document addresses the objective, frequency and scope of the audits, the identity and qualification of the auditor and other related topics. 8.4.3. The related ICP-Brasil entities (AC, AR and PSS), also received prior audit, for accreditation purposes, and that the AC is responsible for carrying out annual audits on these entities, for the purposes of maintaining accreditation, as provided in the document mentioned in the previous paragraph.
8.6. Communication of results	**CP/CPS 8.6**	In accordance with the CRITERIA AND PROCEDURES FOR SUPERVISION OF THE INTEGRATING ENTITIES OF ICP-BRASIL (https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-08-v-4-7-critrios-e-procedimer) and with the CRITERIA AND PROCEDURES FOR PERFORMING AUDITS AT THE INTEGRATING ENTITIES OF ICP-BRASIL(https://www.gov.br/iti/pt-br/centrais-de-conteudo/doc-icp-08-v-4-7-critrios-e-procedimer)
**Also indicate your understanding and compliance with section 3 of Mozilla's Root Store Policy, which says: "Full-surveillance period-of-time audits MUST be conducted and updated audit information provided no less frequently than annually. Successive audits MUST be contiguous (no gaps). .... The publicly-available documentation relating to each audit MUST contain at least the following clearly-labelled information: - name of the company being audited; - name and address of the organization performing the audit; - Distinguished Name and SHA256 fingerprint of each root and intermediate certificate that was in scope; - audit criteria (with version number) that were used to audit each of the certificates; - a list of the CA policy documents (with version numbers) referenced during the audit; - whether the audit is for a period of time or a point in time; - the start date and end date of the period, for those that cover a period of time; - the point-in-time date, for those that are for a point in time; - the date the report was issued (which will necessarily be after the end date or point-in-time date); and - For ETSI, a statement to indicate if the audit was a full audit, and which parts of the criteria were applied, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part1 (General Requirements), and/or Part 2 (Requirements for trust service providers)." **		
8.7. Self-Audits		
9.6.1. CA Representations and Warranties	**CP/CPS 9.6.1**	The CA declares and warrants the following, as well as the requirements of the CA / Browse Forum.
9.6.3. Subscriber Representations and Warranties	**CP/CPS 9.6.3**	9.6.3.1. All information necessary for the identification of the certificate holder must be provided in a complete and accurate manner. By accepting the certificate issued by the CA, the holder is responsible for all information provided by it and contained in that certificate. 9.6.3.2. The CA informs the Root CA of any compromise of its private key and requests the immediate revocation of its certificate.
9.8. Limitations of liability	**CP/CPS 9.8**	The AC is not liable for damages that are not attributable to it or that it has not caused, in accordance with current legislation.

9.9.1. Indemnification by CAs	**CP/CPS 9.9.1**	The AC is liable for any damage that it causes, and is imputable to it, in accordance with the legislation in force, ensuring the right of recourse against the responsible agent or entity.
9.16.3. Severability	**CP/CPS 9.16.3**	The invalidity, nullity or ineffectiveness of any of the provisions of this CPS will not prejudice the other provisions, which will remain fully valid and effective. In this case, the invalid, null or ineffective provision will be considered as unwritten, so that this CPS will be interpreted as if it did not contain such provision, and as far as possible, maintaining the original intention of the remaining provisions.


AC RAIZ
OID: 2.16.76.1.1.0
AC SERPRO SSL
OV SSL Certificate
OID: 2.16.76.1.1.137